

WHAT IS CLAIMED IS:

1 1. A method for accessing a control system in a server from a client
2 computer, wherein the control system includes a logon program to enable the client
3 computer to use a terminal emulation program to logon to the server to access a client
4 process executing in the server to perform control system operations, further
5 comprising:
6 requesting, with the client, security context for the client including
7 authorization to allow the client to access control system functions in the server;
8 returning, with the server, the requested security context to the client; and
9 transmitting, with a client program executing in the client, a control system
10 command and the security context to access the server control system.

1 2. The method of claim 1, wherein requesting the security client
2 comprises the client requesting the server to impersonate the client to obtain the
3 security context, further comprising accessing, with the server impersonating the
4 client, the security context to return to the client.

1 3. The method of claim 2, wherein the Distributed Computing
2 Environment (DCE) protocol is used to provide the client security context, wherein
3 the client uses the sec_login_become_initiator DCE command to request the server to
4 impersonate the client, wherein the server uses the sec_login_become_impersonator
5 DCE command to impersonate the client to obtain the security context.

1 4. The method of claim 1, further comprising:
2 converting, with the server, the security context transmitted through the client
3 program to a pointer to credential information of the client
4 determining from the credential information, with the server, whether the
5 client is authorized to invoke the transmitted control system command; and

6 executing, with the server, the control system command transmitted by the
7 client if the client is authorized to invoke the command.

1 5. The method of claim 1, wherein the client computer includes a
2 different operating system than the server, wherein the client program executing in the
3 client interacts with the client process executing in the server to perform control
4 system operations.

1 6. The method of claim 1, wherein the client requests the security context
2 through a remote procedure call.

1 7. The method of claim 1, wherein the control system is a printing
2 systems manager to control printers and printer related objects managed by the server.

1 8. The method of claim 7, wherein the printer system manager command
2 transmitted by the client comprises a command to reconfigure at least one printer
3 object, thereby allowing the client computer to perform administrative functions.

1 9. A system for accessing a control system in a server from a client
2 computer, wherein the control system includes a logon program to enable the client
3 computer to use a terminal emulation program to logon to the server to access a client
4 process executing in the server to perform control system operations, further
5 comprising:

6 means for requesting security context for the client including authorization to
7 allow the client to access control system functions in the server

1 10. The system of claim 9, wherein the means for requesting the security
2 client comprises the server impersonating the client to obtain the security context,
3 further comprising means for accessing, with the server impersonating the client, the
4 security context to return to the client.

1 11. The system of claim 10, wherein the Distributed Computing
2 Environment (DCE) protocol is used to provide the client security context, wherein
3 the client uses the sec_login_become_initiator DCE command to request the server to
4 impersonate the client, wherein the server uses the sec_login_become_impersonator
5 DCE command to impersonate the client to obtain the security context.

1 12. The system of claim 9, further comprising:
2 means for converting the security context transmitted through the client
3 interface to a pointer to credential information of the client;
4 means for determining from the credential information whether the client is
5 authorized to invoke the transmitted control system command; and
6 means for executing the control system command transmitted by the client if
7 the client is authorized to invoke the command.

1 13. The system of claim 9, wherein the client computer includes a different
2 operating system than the server, wherein the client program is part of the client
3 operating system, and wherein the client program interacts with the client process
4 executing in the server to perform control system operations.

1 14. The system of claim 9, wherein the client requests the security context
2 through a remote procedure call.

a'_{con4}

1 16. The system of claim 15, wherein the printer system manager command
2 transmitted by the client comprises a command to reconfigure at least one printer
3 object, thereby allowing the client computer to perform administrative functions.

1 17. An article of manufacture for use in accessing a control system in a
2 server from a client computer, wherein the control system includes a logon program to
3 enable the client computer to use a terminal emulation program to logon to the server
4 to access a client process executing in the server to perform control system
5 operations, the article of manufacture comprising computer usable media including
6 computer programs embedded therein that cause the client and server computer to
7 perform:

8 requesting, with the client, security context for the client including
9 authorization to allow the client to access control system functions in the server;
10 returning, with the server, the requested security context to the client; and
11 transmitting, with a client program executing in the client, a control system
12 command and the security context to access the server control system.

1 18. The article of manufacture of claim 17, wherein requesting the security
2 client comprises the client requesting the server to impersonate the client to obtain the
3 security context, further comprising accessing, with the server impersonating the
4 client, the security context to return to the client.

1 19. The article of manufacture of claim 18, wherein the Distributed
2 Computing Environment (DCE) protocol is used to provide the client security
3 context, wherein the client uses the sec_login_become initiator DCE command to

4 request the server to impersonate the client, wherein the server uses the
5 `sec_login_become_impersonator` DCE command to impersonate the client to obtain
6 the security context.

1 20 The article of manufacture of claim 17, further causing the server to
2 perform:
3 converting the security context transmitted through the client program to a
4 pointer to credential information of the client;
5 determining from the credential information whether the client is authorized to
6 invoke the transmitted control system command; and
7 executing the control system command transmitted by the client if the client is
8 authorized to invoke the command.

1 21. The article of manufacture of claim 17, wherein the client computer
2 includes a different operating system than the server, wherein the client program
3 executing in the client interacts with the client process executing in the server to
4 perform control system operations.

22. The article of manufacture of claim 17, wherein the client requests the security context through a remote procedure call.

1 23. The article of manufacture of claim 17, wherein the control system is a
2 printing systems manager to control printers and printer related objects managed by
3 the server.

1 24. The article of manufacture of claim 23, wherein the printer system
2 manager command transmitted by the client comprises a command to reconfigure at

-18-

inter object, thereby allowing the client to use the same functions.

Figure 1

- at
cont